UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,996	02/12/2002	Chang-Ping Lee	2222.5390005	7160

26111 7590 08/20/2008

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/074,996	LEE ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/2/08*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *2/12/02* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1,2, and 4-56 have been considered but are moot in view of the new grounds of rejection.

2. As per claims 11 and 40, it is argued by the applicant that Hirano fails to disclose "that security information that includes access rules and a file key is encrypted with a user key and the file is encrypted with the file key". The examiner disagrees with the applicant's assertion, Hirano discloses of using user consent information which serves as a key to encrypt the contents key. The consent information, which includes the access rules, encrypts the contents key by using the user information and the user information is required to obtain the contents key, see column 7, line 64 through column 8, line 2 and column 8, line 60 through column 9, line 10.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1,2,4-10,20-31,33-42,45-51, and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirano et al, U.S. Patent 7,046,807 in view of Laczko, Sr et al.

As per claims 1,24,51 and 54, it is disclosed by Hirano et al of a method and a software product for securing a file, the method comprising determining, in an operating system supporting the application, whether the file being accessed is secured when a request to access the file is received, when the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application, when the file is determined to be non-secured, loading the file into the application without activating the cipher module and launching an application when the request to access the file is received (col. 5, lines 3-23 and col. 7, line 55 through col. 8, line 2). The teachings of Hirano et al fail to disclose that the cipher module, once activated, operates transparently to a user requesting an access to the file. It is disclosed by Laczko et al of a cipher module operating transparently to a user while when request access to a file (col. 12, line 66 through col. 13, line 11). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to make encryption operations transparent to a user. The teachings of Laczko et al disclose of motivation for allowing the encryption and decryption operations to occur transparently by reciting that a small amount of additional processing capacity of a processor is required (col. 13, lines 7-11). It is obvious that the teachings of Hirano et al could have used the cipher module operating transparently to a user by ensuring that a minimal amount of processing power is used by a processor as is taught by Laczko et al.

As per claim 2, Hirano et al teaches that the cipher module, once activated, operates within the operating system (col. 7, line 55 through col. 8, line 2).

As per claims 4 and 25, Hirano et al teaches that the secured file includes a header and an encrypted portion, the header including or pointing to security information including a file key that, once obtained, can be used to decrypt the encrypted portion (col. 5, lines 3-23).

As per claims 5 and 26, Hirano et al discloses of determining of whether the file being accessed is secured comprises determining if the file being accessed includes the header (col. 5, lines 3-23).

As per claim 6, Hirano et al teaches that the header further includes a flag indicating that the file being accessed is secured, and wherein the determining of whether the file being accessed is secured comprises determining if the file has the flag (col. 5, lines 3-23).

As per claims 7 and 27, the teachings of Hirano et al recite wherein the loading of the file through the cipher module into the application comprises retrieving the file key, decrypting the encrypted portion with the file key in the cipher module, and sending the file in clear mode to the application (col. 7, line 55 through col. 8, line 2).

As per claims 8 and 28, it is disclosed by Hirano et al that the security information including the file key is encrypted with a user key, and wherein the retrieving of the file key comprises obtaining a user key associated with a user requesting an access to the file, and decrypting the encrypted security information with the user key to retrieve the file key (col. 7, line 55 through col. 8, line 2).

As per claims 9 and 29, Hirano et al discloses that the security information further includes access rules controlling how and who the secured file can be accessed (col. 5, lines 3-23).

As per claims 10 and 30, the teachings of Hirano et al recite wherein the loading of the file through the cipher module into the application only happens when access privilege of the user is within permissions granted by the access rules (col. 5, lines 3-23).

As per claims 20 and 53, Hirano et al discloses a method for providing access control to a file in an application, the method comprising forwarding the request to a access the file to a file system manager in the operating system, activating a document securing module by the file system manager to determine whether the file being accessed is secured, activating a cipher module when the file is determined to be secured, and loading the file through the cipher module into the application and launching an application that access the file (col. 5, lines 3-23 and col. 7, line 55 through col. 8, line 2). The teachings of Hirano et al fail to disclose that the cipher module, once activated, operates transparently to a user requesting an access to the file. It is disclosed by Laczko et al of a cipher module operating transparently to a user while when request access to a file (col. 12, line 66 through col. 13, line 11). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to make encryption operations transparent to a user. The teachings of Laczko et al disclose of motivation for allowing the encryption and decryption operations to occur transparently by reciting that a small amount of additional processing capacity

of a processor is required (col. 13, lines 7-11). It is obvious that the teachings of Hirano et al could have used the cipher module operating transparently to a user by ensuring that a minimal amount of processing power is used by a processor as is taught by Laczko et al.

As per claim 21, Hirano et al recites of retrieving security information from the file when the file is determined to be secured, the security information including a file key and access rules, and obtaining an access privilege of a user requesting to access the file (col. 5, lines 3-23).

As per claim 22, the teachings of Hirano et al recite wherein the activating of the cipher module proceeds successfully when the access privilege is within permissions granted by the access rules (col. 6, lines 33-45).

As per claim 23, it is disclosed by Hirano et al wherein the activating of the cipher module comprises decrypting an encrypted portion of the secured file with the file key (col. 7, line 55 through col. 8, line 2).

As per claims 31 and 55, Hirano et al teaches of a software product including computer instructions for securing a file, the instructions, when executed by a processor, cause the processor to perform operations of maintaining a file key in a temporary memory space, encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and storing, in a storage space, a secured file including the encrypted file and a header, wherein the header includes or points to security information including the file key and launching an application (col. 5, lines 3-23 and col. 7, line 55 through col. 8, line 2). The

teachings of Hirano et al fail to disclose that the cipher module, once activated, operates transparently to a user requesting an access to the file. It is disclosed by Laczko et al of a cipher module operating transparently to a user while when request access to a file (col. 12, line 66 through col. 13, line 11). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to make encryption operations transparent to a user. The teachings of Laczko et al disclose of motivation for allowing the encryption and decryption operations to occur transparently by reciting that a small amount of additional processing capacity of a processor is required (col. 13, lines 7-11). It is obvious that the teachings of Hirano et al could have used the cipher module operating transparently to a user by ensuring that a minimal amount of processing power is used by a processor as is taught by Laczko et al.

As per claim 33, Hirano et al teaches wherein the encrypting of the file with the file key happens whenever the file is caused to be stored in the storage space (col. 5, lines 3-23).

As per claim 34, Hirano et al recites wherein the encrypting of the file with the file key happens upon receiving an instruction from the application or an operating system supporting the application (col. 5, lines 3-23).

As per claim 35, Hirano et al teaches wherein the instruction is one of (i) Save, (ii) Close and (iii) Exit, all provided in the application (col. 5, lines 3-23).

As per claim 36. Hirano et al discloses wherein the instruction is generated from an automatic operation of saving the file being opened into the storage space, the

automatic operation is either triggered by the application itself or the operating system (col. 5, lines 3-23).

As per claim 37, Hirano et al discloses wherein the security information further includes access rules of how and who the secured file can be accessed (col. 6, lines 33-45).

As per claim 38, it is taught by Hirano et al of encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group (col. 5, lines 3-23).

As per claim 39, Hirano et al recites of attaching the header to the encrypted file, wherein the header includes the security information encrypted in addition to a flag indicating that the file is secured (col. 5, lines 3-23).

As per claims 40 and 56, Hirano et al teaches of a computing device for securing a file in an application environment, the computing device comprising an application, when executed, accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted version of the file, a cipher module activating upon determining that the file being accessed is secured, wherein the security information is encrypted and can be decrypted with a user key when authenticated; and wherein the file key can be retrieved to decrypt the encrypted portion only after the access rules have successfully measured against access privilege of the user and launching an application to access the file (col. 5, lines 3-23 and col. 7, line 55 through col. 8, line 2).

As per claim 41, Hirano et al discloses of an operating system supporting operations of the application, and wherein the cipher module is embedded in the operating system (col. 7, line 55 through col. 8, line 2).

As per claim 42, Hirano et al discloses wherein the cipher module operates in a path through which the file is caused to pass when accessed by the application (col. 7, line 55 through col. 8, line 2).

As per claim 45, Hirano et al teaches wherein the user key becomes authenticated only when the user is authenticated by an authentication process to verify who the user claims to be (col. 10, lines 12-35).

As per claim 46, Hirano et al discloses wherein the computing device is coupled to another computing device over a data network, the user key becomes authenticated only after the user is successfully logged from the computing device into the another computing device (col. 10, lines 12-35)

As per claim 47, Hirano et al teaches wherein the computing device is provided with means for capturing biometric data of the user, the user key becomes authenticated only after the biometric data is successfully verified to support who the user claims to be (col. 10, lines 12-35).

As per claim 48, it is taught by Hirano et al wherein the user key becomes authenticated after the computing device receives credential information from the user (col. 10, lines 12-35).

As per claim 49, Hirano et al discloses wherein the credential information includes one of a password entered by the user, biometric information of the user, personalized information about the user (col. 10, lines 12-35).

As per claim 50, Hirano et al recites wherein the biometric information is captured from a device coupled to the computing device (col. 10, lines 12-35).

5. Claims 11-19,32,43,44, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirano et al, U.S. Patent 7,046,807 in view of Novak, U.S. Patent 6,865,555.

As per claims 11 and 52, Hirano et al teaches of a method for securing a file, the method comprising encrypting the file with the file key in a cipher module to produce an encrypted portion, preparing security information for the encrypted portion, the security information being encrypted with a user key and including the file key and access rules to control access to the encrypted portion, and attaching the encrypted security information to the encrypted portion and launching an application that accesses the file (col. 5, lines 3-23; col. 7, line 55 through col. 8, line 2; and col. 8, line 60 through col. 9, line 10). The teachings of Hirano et al fail to disclose of maintaining a file key in a temporary memory space. It is taught by Novak of maintaining a file key in a temporary memory space (col. 12, lines 16-28). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to applying the storage of a key in temporary memory space. The teachings of Novak disclose of motivation for doing so by reciting that the data is stored temporarily in order to avoid

tampering (col. 8, line 66 through col. 9, line 8 and col. 12, lines 20-24). It is obvious that the teachings of Hirano et al would have been more secure by temporarily storing a file key in order to avoid tampering as taught by Novak.

As per claim 12, Novak teaches of deleting the file key from the temporary memory space when the attaching of the encrypted security information to the encrypted portion is complete (col. 12, lines 16-28). Please refer above for the motivation and reasons of applying the teachings of Novak to the disclosure of Hirano et al.

As per claim 13, Hirano et al discloses that wherein the encrypting of the file with the file key, the preparing of the security information, and the attaching of the encrypted security information happen whenever the file is caused to be stored in a storage space (col. 14, lines 18-35).

As per claim 14, it is disclosed by Hirano et al wherein the encrypting of the file with the file key, the preparing of the security information, and the attaching of the encrypted security information happen upon receiving an instruction from an application or an operating system supporting the application (col. 5, lines 3-23).

As per claim 15, Novak teaches wherein the application is provided in Microsoft Office and the operating system is Microsoft Windows (col. 9, lines 30-32). Please refer above for the motivation and reasons of applying the teachings of Novak to the disclosure of Hirano et al.

As per claim 16, it is disclosed by Hirano et al that the instruction is one of (i) Save, (ii) Close and (iii) Exit, all provided in the application (col. 5, lines 3-23).

As per claim 17, Hirano et al teaches that the instruction is generated from an automatic operation of saving the file being opened into the storage space, the automatic operation is either triggered by the application itself or the operating system (col. 6, lines 33-45).

As per claim 18, Hirano et al recites of encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group of users (col. 5, lines 3-23).

As per claim 19, Hirano et al teaches wherein the access rules in the security information comprises user information identifying who can assess the encrypted portion and how the encrypted portion can be accessed (col. 5, lines 3-23).

As per claim 32, Hirano et al fails to teach of deleting the file key from the temporary memory space when the application is caused to close the file . Novak discloses of deleting the file key from the temporary memory space when the application is caused to close the file (col. 12, lines 16-28). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to applying the storage of a key in temporary memory space. The teachings of Novak disclose of motivation for doing so by reciting that the data is stored temporarily in order to avoid tampering (col. 8, line 66 through col. 9, line 8 and col. 12, lines 20-24). It is obvious that the teachings of Hirano et al would have been more secure by temporarily storing a file key in order to avoid tampering as taught by Novak.

As per claim 43, the teachings of Hirano et al fail to disclose of maintaining a file key in a temporary memory space. It is taught by Novak of maintaining a file key in a

temporary memory space (col. 12, lines 16-28). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to applying the storage of a key in temporary memory space. The teachings of Novak disclose of motivation for doing so by reciting that the data is stored temporarily in order to avoid tampering (col. 8, line 66 through col. 9, line 8 and col. 12, lines 20-24). It is obvious that the teachings of Hirano et al would have been more secure by temporarily storing a file key in order to avoid tampering as taught by Novak.

As per claim 44, it is disclosed by Novak wherein the file key is deleted from the memory space as soon as the file is wrote back to the storage space (col. 12, lines 16-28). Please refer above for the motivation and reasons of applying the teachings of Novak to the disclosure of Hirano et al.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2131